

CyberTalents Challenges

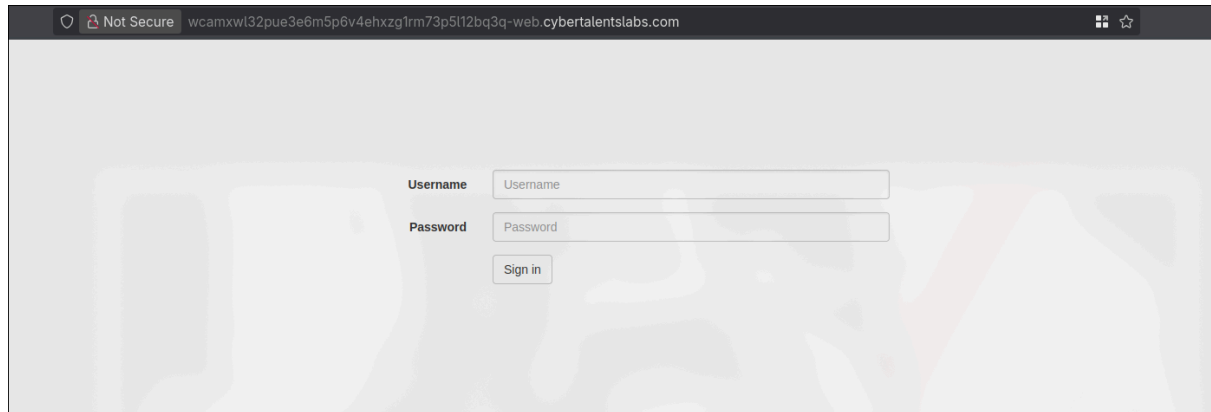
Web Security – Admin has the power – level easy

Author: levith4n

Description:

Administrators only has the power to see the flag , can you be one ?

Pertama, ini adalah tampilan awal dari aplikasi web. Seperti yang terlihat, kita ditampilkan sebuah *form login*.

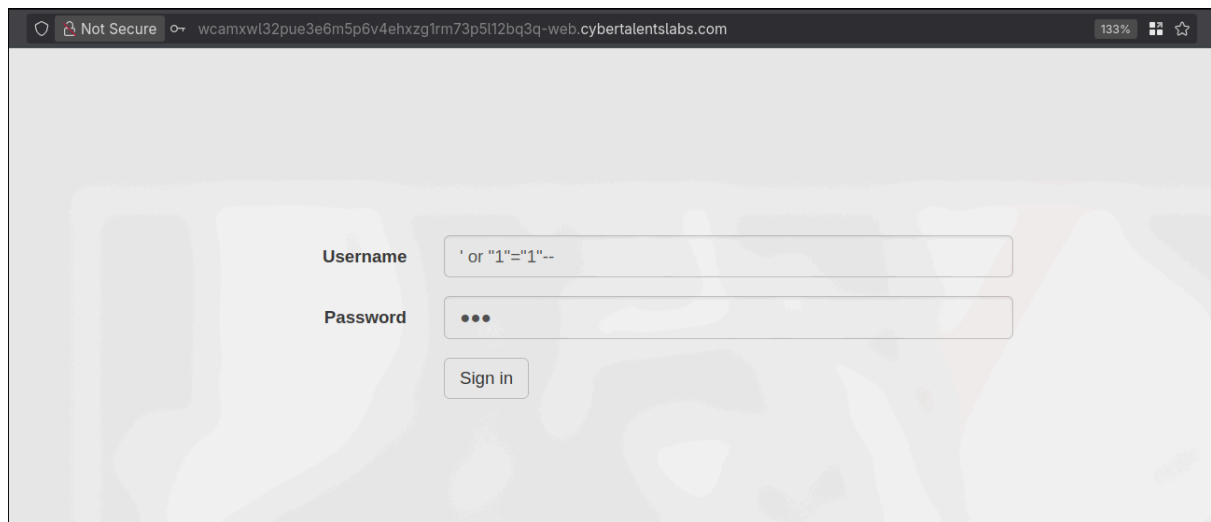


Not Secure | wcamxwl32pue3e6m5p6v4ehxzg1rm73p5l12bq3q-web.cybertalentslabs.com

Username

Password

Saya mencoba untuk melakukan *SQL Injection authentication bypass*.

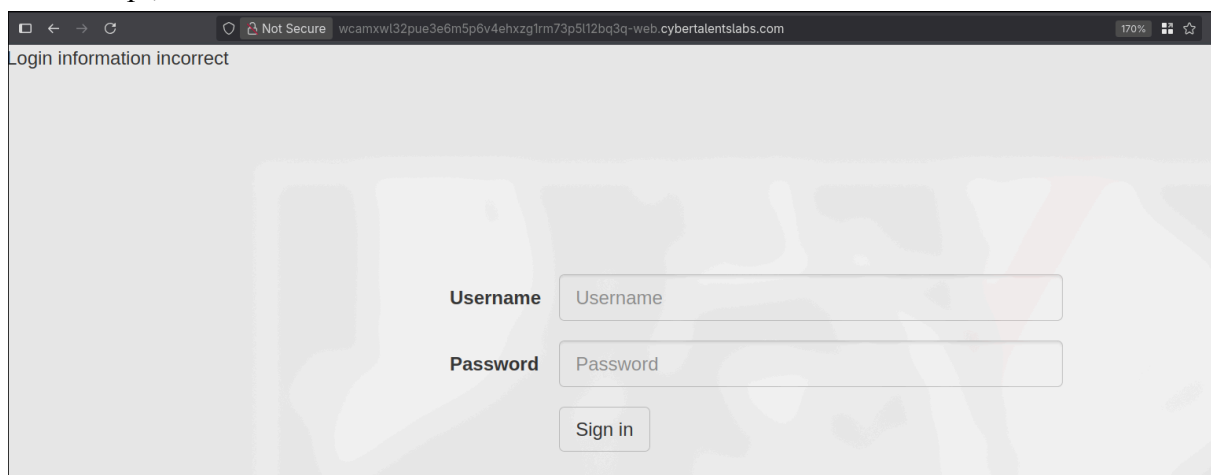


Not Secure | wcamxwl32pue3e6m5p6v4ehxzg1rm73p5l12bq3q-web.cybertalentslabs.com 133%

Username

Password

Akan tetapi, hal ini tidak berhasil.



Not Secure | wcamxwl32pue3e6m5p6v4ehxzg1rm73p5l12bq3q-web.cybertalentslabs.com 170%

Login information incorrect

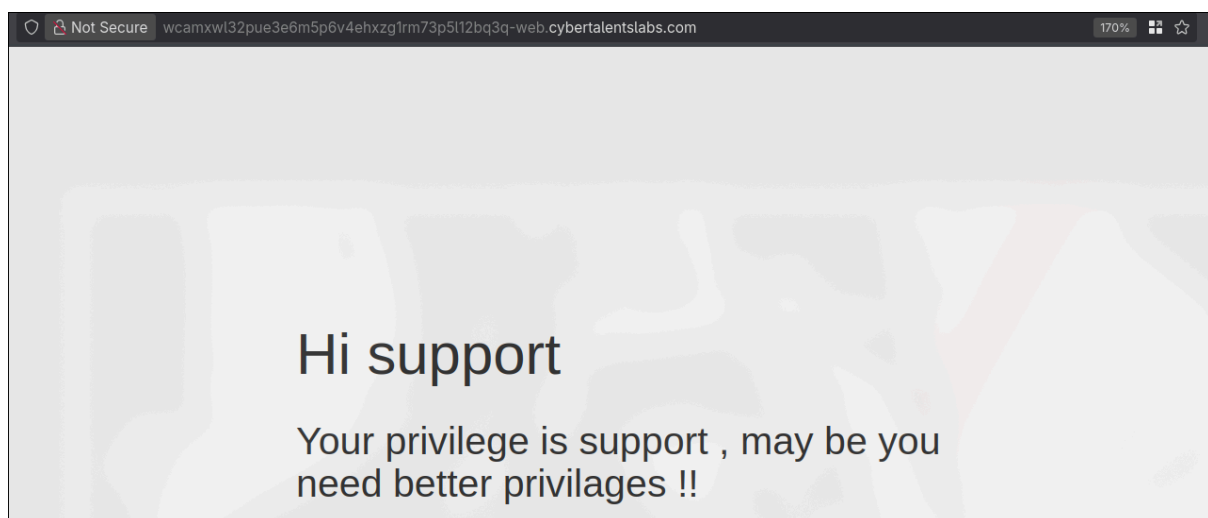
Username

Password

Kemudian, saya mencoba untuk melakukan pengumpulan informasi, dimulai dari membaca *source code*. Saya menemukan sebuah *comment* yang berisi kredensial.

```
1 Login information incorrect<!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta charset="utf-8">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <!-- The above 3 meta tags *must* come first in the head; any other head content must come *after* these tags -
8 <title>Admin Panel</title>
9
10 <!-- Bootstrap -->
11 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="
12
13 <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
14 <!--[if lt IE 9]>
15 <script src="https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js"></script>
16 <script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
17 <![endif]-->
18 <!-- TODO: remove this line , for maintenance purpose use this info (user:support password:x34245323)-->
19 </head>
20 <body>
21 <div class="container" style="padding-top: 150px;">
```

Saya langsung mencoba *login* menggunakan kredensial tersebut dan berhasil masuk ke *dashboard*. Akan tetapi, terdapat pesan “Your privilege is support, may be you need better privileges!!”, pesan ini memberikan saya *hint* apakah ada *broken access control* pada aplikasi web ini.



Saya mencoba meng-*intercept traffic* saat pada halaman *dashboard* ini. Seperti yang terlihat pada *request header Cookie*, terdapat **role** yang mengindikasikan kita login sebagai role apa.



Saya pun langsung mencoba mengganti **role** menjadi **admin** dan seperti yang terlihat saya berhasil mendapatkan flag.

